Vorwort

Das vorliegende Buch richtet sich an Leser, die

- die Rolle eines IT-Sicherheitsbeauftragten oder IT Security Managers übernommen haben bzw. in Kürze übernehmen werden,
- in einer Sicherheitsabteilung oder im IT-Bereich tätig sind,
- generell für Sicherheitsbelange einer Organisation verantwortlich sind, oder
- sich einfach nur in das interessante Gebiet der Informationssicherheit einarbeiten möchten.

Die Informationssicherheit als Fachgebiet ist z. T. unter anderen Überschriften wie

- IT-Sicherheit (IT Security),
- Datensicherheit oder
- Informationsschutz

bekannt und berührt auch Themen wie den Datenschutz, den Geheimschutz (mit dem Unterthema Data Leakage Prevention, DLP), das Qualitätsmanagement, das Compliance Management bzw. die Ordnungsmäßigkeit der Datenverarbeitung, d. h. Informationssicherheit ist ein *interdisziplinäres* und *querschnittliches* Thema.

Die Informationssicherheit entwickelt sich beinahe ebenso schnell wie die IT insgesamt, da sie sich permanent auf neue technologische Gegebenheiten, deren Anwendungen und Bedrohungen einstellen muss. Wer in dieses dynamische Gebiet einsteigt, kann deshalb schnell den Überblick verlieren – aber auch nach vielen Jahren Berufserfahrung immer wieder Neues entdecken. Dennoch gilt es gerade zu Beginn, sich auf das Wesentliche zu konzentrieren.

Im Grunde muss sich heute jede Organisation[1], die schützenswerte Informationen besitzt und Daten sicher verarbeiten will, mit diesen Fragen beschäftigen: Informationssicherheit ist zu einem wichtigen Faktor der *Vorsorge* geworden. Dabei hat jede Organisation mehr oder weniger eigene Erfahrungen mit diesem Thema gemacht – oft in der Rolle

[1] Unternehmen, Behörde, Verband, Verein usw.

des Geschädigten. Aus diesem Grund muss man für Informationssicherheit nicht mehr besonders werben; wir ersparen uns deshalb auch, alle möglichen Horror-Szenarien zu beschreiben – man kennt sie hinlänglich aus entsprechenden Publikationen. Vorrangig sollen hier die Fragen behandelt werden,

- mit welcher Strategie man das Thema angeht,
- wie viel Sicherheit[2] wirklich benötigt wird,
- wie man die gewünschte Sicherheit erreichen, überprüfen und aufrechterhalten kann,
- wie man die Sicherheit laufend an die Geschäftserfordernisse anpasst,
- wie man gegenüber Partnern, Kunden, Aufsichtsbehörden und Banken die eigene Sicherheit nachweisen kann,
- ob es einen *Return on Security Investment* (RoSI) gibt und wie man ihn ggf. erreicht.

In vielen Organisationen haben solche Fragestellungen dazu geführt, dass ein Sicherheitsmanagement eingerichtet worden ist, das sich in Gestalt eines *IT Security Managers* bzw. *IT-Sicherheitsbeauftragten* oder eines entsprechenden *Sicherheitsgremiums* der Thematik annehmen soll.

Eine zentrale Funktion übernimmt dann neben der *Sicherheitsleitlinie* das so genannte *Sicherheitskonzept*, in dem alle Analysen und Entscheidungen, die die Informationssicherheit betreffen, enthalten sind. Um dieses meist umfangreiche Dokument rankt sich in der Praxis ein ganzes Bündel von begleitenden Dokumenten – sehr zum Leidwesen der Beteiligten, da „Paperware“ einerseits Schwerstarbeit ist und andererseits allein noch gar nichts bringt.

Inzwischen sind mit der Normenreihe ISO 27000 und dem IT-Grundschutz zwei Vorgehensmodelle für die Sicherheitskonzeption quasi gesetzt, d. h. in den meisten Fällen fällt die Wahl auf eine der beiden Methoden, die bei genauer Betrachtung viele Gemeinsamkeiten haben.

In der Praxis bleibt das Erstellen von aussagekräftigen, anwendbaren und zielführenden Sicherheitskonzepten dennoch ein Kardinalproblem: Individuelle Risiken, die Wirksamkeit von Gegenmaßnahmen und das verbleibende Restrisiko können meist nicht berechnet, sondern bestenfalls aus der Erfahrung *geschätzt* werden.

Dass bei den Gegenmaßnahmen eine schier unerschöpfliche Auswahl besteht, sogar umfangreiche Kataloge existieren, in denen die Bereiche Recht, Organisation, Personal, Technik und Infrastruktur akribisch behandelt werden, macht die Sicherheitskonzeption nicht unbedingt leichter – vor allem, wenn es darum geht, die Eignung, Wirksamkeit und Wirtschaftlichkeit einzelner Maßnahmen *in einem speziellen Einsatzszenario* zu bewerten.

„Alle“ Sicherheitsmaßnahmen umfassend und detailliert zu behandeln würde den Rahmen dieses Buches sprengen. Es musste deshalb eine Auswahl getroffen werden: Als

[2] Wir verwenden der einfacheren Lesbarkeit wegen das Wort *Sicherheit* stellvertretend für IT-Sicherheit, Informationssicherheit etc. – solange keine Missverständnisse zu befürchten sind.

Orientierung dienten mehrtägige Seminare zum Thema Informationssicherheit, die die Autoren in den vergangenen Jahren zahlreich durchgeführt haben und noch durchführen. Das Feedback der Teilnehmer hat dabei vielfältige Anregungen zur Überarbeitung von Methodik und Didaktik gegeben.

Aktualisierungen Für diese vierte Auflage wurden die aktuellen Entwicklungen der ISO 2700-Reihe, insbesondere die Neufassung der ISO 27001, berücksichtigt. Diese Normenreihe ist für viele international agierende Unternehmen inzwischen unverzichtbar geworden; ihre Umsetzung und Einhaltung wird im internationalen Wettbewerb oft schon vorausgesetzt.

Neben einer Aktualisierung aller Kapitel wurde als neues Thema die Verhinderung von unerlaubten Datenabflüssen (Data Leakage Prevention) aufgenommen (Kap. 12) sowie an vielen Stellen Sicherheitsaspekte beim Einsatz mobiler IT-Systeme berücksichtigt.

Eine größere Überarbeitung hat auch das Kapitel „Grundstrukturen“ erfahren, das jetzt als Kapitel 2 vor allem dem schwierigen, aber unerlässlichem Arbeitsschritt der *Inventarisierung* gewidmet ist.

Danksagung In dieses Buch sind viele Kritiken und Vorschläge der Leser früherer Auflagen eingeflossen: hierfür herzlichen Dank.

Dem Springer-Verlag und seinem Lektorat danken die Autoren für die professionelle Unterstützung bei der Neuauflage dieses Buches.

Im Juli 2015 Dr. Heinrich Kersten, Dr. Gerhard Klett

http://www.springer.com/978-3-658-09973-2

Der IT Security Manager
Aktuelles Praxiswissen für IT Security Manager und IT-Sicherheitsbeauftragte in Unternehmen und Behörden

Kersten, H.; Klett, G.

2015, XX, 297 S. 24 Abb., Softcover
ISBN: 978-3-658-09973-2